Okay folks I understand that this is the panel session between you and lunch so will take every opportunity to work through lunch if necessary to give you the information that you so desire. Industry is always as I mentioned in my comments yesterday is always willing and ready to speak to the customers and tell him everything you ever wanted to know about smart cards. The problems is, is trying to speak in the same language because we speak in terms of bits and bytes and use lot of acronyms and words that are native to our world and you are trying to interrupt that in terms of what does this mean to me, how do I just issue a card, how do I be compliant with these new rules and regulations, how do a I manage it within our process, in our system and somehow we have to try to bridge that gap and try to find a common ground and that really went into a lot of decision making that I made in terms of selecting that the three people that are going to speak on this panel today because starting in my fare left, ____ is truly one of the founding members of this industry in terms of smart card technology and _____ an integral part of the smart card _____ organization as an educator. Two individuals who may be seen in this technology for the first time and he is done a terrific job in past for us in terms of putting in terms that we can hopefully understand at some level together.

_____ is one the chair people of a new group that formed called the physical access council and we have a combination of government and industry working together to develop some really useful information and knowledge base about the implementation of smart cards particularly as it applies to physical access which is one of the important components of what the PIV implementation is going to involve and _____ is going to give us some of the perspective of implementing PIV in physical access environments in some other work that is going on within the physical access council to help support those efforts and provide you with the resources that you need and last but not least, Stephen Howard here has got a tremendous amount of background experience in photography, PKI, and implementing smart cards in th area of logical security and Steve was also as well as the three of these gentleman heavily involved in the process that have gone on in the last six months in working through the _____ documents the special publications and trying to provide an industry voice to this process so that we all get to an end game that we feel we can be comfortable with so without taking anymore time away I want to go to the next slide. These would be the individuals that I just introduced and the contact information, that information will also be at the end of the presentation as well so if any of you want to followup after this conference with the discussion, you will be able to do that. I also wanted to mention before I will lost the opportunity that the smart card _____ puts on educational workshops, it is one of the things we do to try to help support this industry and if you feel that you still need more information and more education about how we implement smart cards in the government, the smart card ______ wants to be able to provide you that opportunity so based on the feed back what we get from this workshop and the following workshops in the next few weeks, we will make a determination about scheduling full day or two day workshop to get into more of the application and implementation details of the technology so that you can _____ with what you heard in the last day in half in terms of policies and the rules and the regulations to go on. So let me please start with _____ I just forget there was one other to just to go over, what we are going to cover in these three sessions _____ is going to talk a little bit about the standards and smart cards, _____ where we have come from and where we are at today followed by Steve who is going to get into the PIV data model and when and what to use back in the PIV and then _____ will go ____ talking about the PIV card and the implementation for physical access

Thank you

It is a challenge to talk about smarts cards and standards after GM presentations so I will not talk bits and bytes don't worry about it, but I thought that you needed some backgrounds on standards so I thought about starting in the beginning. I am going back to genesis about smart card and standards so I am not going to bore you about _____ or te books which have written after that part just remember that _____which was at the origin was not enough and _____that's where it started, so we had a problem, it was not interoperable.

So in the land of North America we decided to go for _____ and to have something which was really _____ interoperable. It is important to notice here that we add interoperable _____ we had framework to develop applications, but didn't have enough guidance to get one application working between agencies that is the part which was missing, but that is framework and we will come back on that word a little later. I am going pretty fast because of time I think, the two are the presenters are moving important than standards.
So in the quest for _____ there was a requirement for PIV to really interoperate in order provide security, that is all those _____. Now we still are missing a global application framework for development and that is why I am mentioning two other things which are happening just for you to understand how all these things are going to fit together. At the international level, there is _____ development for interoperability between applications, its framework which will allow us to understand the differences and at the end to understand each other, very high level framework so we SP-80073 is an application specification _____,it is something which defines the rules of the application to interoperate, but be careful if you want to add other applications on the cards which will have that one, you are outside of this specification, you still need another framework to work with so there will be a lot of challenges for people issuing with that specification if they want to add something in their card. From the standard stand point there is one development which is _____ and there is an effort which is going to happen that I am going mention in the the next _____. The heart of interoperability for application is that you need a _____model. This has been achieved in _____for the PIV application. But the naming convention which were mentioned by Jim do not allow to expand to other applications without some more work being done, that is still to be done for other applications. I am trying to define the _____ what you need to do. The commands and function have been mailed out. This is now easy to do much simpler than before. We know the tools, we know how to talk to the card, we now that is pretty well done. Limited number of cards interfaces, we just don't have as many options as we had before, it was _____, nightmare just a complete menu without guidance. We don't have that problems anymore. Now we just have the tip of the iceberg, that were the problem starts. As Phil has been mentioning the rest of the system, the back end is under the level of under the level of the water, you still have to deal with it. The card is what you see, the

card is what is going to be out there that is the easy part to do. You will _____some vendor is showing up with _____ is compliant. I hope the reference model is going to define that a little better, but it is easy part to do and just like for an iceberg its about a tenth of what needs to be done. The rest is still under the water and you will have and it was question which was very good question how to use it, that is still to be defined you will still have to built on those things there. So the application itself is more complex and if you want to put applications in the same card you will have to ask yourself about what do I do which _____do I turn to, which framework do I decide to play with, that is not going to be an easy answer at this point in time. All the issuance in the security and we have seen that about credential is a daunting task, do not under estimate that if not because you have got the card that you are going to save you from that problem and ____ system on the way for them to cooperate.

Inorder to verify that the _____ is still valid is also something which is not trivial. Buying cards without knowing the applications, just like buying a car without knowing the roads, so be careful about what you are going to do down there. So from the standard standpoint who is working on the solution and what is going on. Because I think that is important message you need to get from this presentation here. Some more work is required, I was very happy to hear that June 25 for the reference implementation is now getting there, so that is pretty good. I was a little less happy that teams question was not answered, but that is another one anyway. There is an international effort which is led by _____ and thanks to _____ by a lot of people involved down there, which we will allow not only PIV cards, but a lot of other applications which are going to be developed using smart cards to interoperate to really understand each other, just like if you go into a conference, _____ you first need to decide, which kind of language you are going to use. Most of the times it is English, but it is not always the case so you have got to be careful about how to do it. That is what ______ is all about. It is moving along, there is lot of interest from the International Community and believe it or not _____ is the framework which initiated that works, so the US has been proceed as a leader in that matter. That is very good news. We are now very active at the US level in the international standard and we are getting a lot of recognition for the work, which has been down, thanks to all of you implementers and users of that technology. Now locally in the _____ work _____ is working for bridge, a kind of solution which will allow this framework for applications to be developed and co-exists with _____card. That is the next step, that is happening now, if you have nothing else to do please join _____ come and work on that subject. Because there will be a lot of work to do in that area so it is to allow PIV to co-exists, to allow other applications to be coherent, it is to allow the framework of applications which are going to be built on those tools to really live together and to be in global understanding of national systems, that is what this work is going to be. It has just started in the next 30 days. There should be a recommendation from an another group which was _____ yesterday on these matters. So the delicate choice that you are going to face now is do you want a _____ where you are _____ lot of applications and in order to that you need a frame work to bill those applications on that _____ or you want a card which is end phase just for the PIV application. I am just over simplifying the choices. Those two elements are going to be available. It is possible to have the end state application on _____ that is also possible and thanks to the way 873 has been written. This is possible. But you will have to make the choices about applications and cards and other applications in the same framework. It is another simple choice at that point, but has not been clearly defined. The new solution for cards is probably a better interoperable system, but until compliant test is defined, just be careful about what you are going to put your fingers in because everybody reads _____ and the implementations are sometimes very interesting. You know engineers are very creative and they can find a lot of solutions from the same document. That is the choice I was talking about, you have got the transitional, we know the flaws or at least a lot of them, but we know how to make it work and thanks to the data model, we have the way now to interoperate at the data model level. Keep that in mind, that is something, which is a fact. We would not be able to test it thought, that is where the problem is. The other new solution here is easier to work with new applications, we will take advantage of the new cards, but it is the new system. It is a new line of thought, which has now been completely transpose to other applications, so they are some _____ there. It will be solved, both _____ are _____. You will have products _____ and it will be mention there. That is all for ____ and I hope I was not too boring and I am just waiting for the revelation to be able to write the last books of the whole story, so we are working on it.

Thank you.

What a fantastic intro! So I was asked to come up and follow this. Okay, now you know the basic framework and the standards and how the application may behave and as you all said one of the things that everybody is very proud of between the _____ and _____ and all the work that was done is the fact that we do have a _____ and that is true strategic advantage, because it means that the business applications you write are not going to go _____ depending on which one you worked on, either transitional or end state. The basic behaviors do not change, so your real investment that 90% problem we keep talking about does not get lost in the fold. So lets go over the structure of the data model really quickly. This is explicitly what is defined 800-73 very quickly, it is the card capability container that let you determine discovery process, what kind of card, what type of card, what version of card. We go into the card holder _____ ID, the first required certificate and keep _____ which is for _____ authentication, the finger prints, printed information, if it is printed on the card it is in the chip and the reason for that is we are adding an additional security element that stops fraud by signing that, which is on the chip. So if I have the surface of the card that is modified and then I read the chip, I am going to see a difference and I am going to be able to prove it. So it is a strategic advantage from both forensic and terrorist exploitation restrictions and then we have the cardholder _____ image, same basic idea, but it is also to allow for alternative methods of verifying who you are in case you do not have digits. That is the strategic concern. The optional key _____ the security object, want to add this, this is something _____ just talked about and it is a very strategic part of discussion and I _____. This is the federal versus the state. Okay, so we have a standard, _____ you shall do the following things. They are the mandatories that you must do, but it does not restrict issuers from adding additional applications in data. Yes there are some technology things that we talked about, but fundamentally this is entirely capable based on the PIV definition, so specifically the DOD environment, they have demographic information buffers and that is a very strategic advantage. There are a lot of cases where they are off line, Bosnia, Iraq. They are not able to talk to _____ system, so how do I transfer who you are to that new local system. That is the obligation of the chip, it allows us to have that information on the card, that is a pretty cool feature to have. Other things like _____ or the use of _____ biometrics or the card capability and security object in the contact list domain. They are not defined in PIV, but you are not restricted from taking advantage of it. But when we do that those are issuer's specific applications in data and they are not considered interoperable. They are a great way to test in concert with PIV, how I might do this and there are lot of instances in particular with operating systems like Java card and _____ where they have always had, what we call private extensions and there are the mechanism for proving that this is a good methodology and it is the way you want to work in the future and as soon as people have enough belief in how you are moving forward, then we migrated into the major application. So it allows the capability to move ahead. I am not going to talk about this and I just wanted to highlight it. When we look at the data model on the card that is the _____, the real issue is how we are going to the back end transactions to validate things. 873 defines _____ for operational use cases. It does require those back end transactions. I really wanted to focus on the structure and the support of the data model here and how you would use it and will call an operational sense, when I actually receive a card what I do I do with it. All right so as apposed to all the things I am going to do on the back end approves its all the other things, just simply what is the card capable of. So another way of putting this, when do I use what. How do I make sense of it for real applications. So there are really three basic things that we have to worry about. The first thing when I want to register your credential into a system to take advantage of the fact that the credential is available. So somebody issued a card that is kind of cool. I have an identity and I have a capability, but now I want to use it in physical or a logical access system, that is a registration process in the first sense.

So when we look at the registration, where is the stuff you need, so the first thing will be what is my credential number, all right. That is buried in the cardholder unique ID. It is part of the federal agency's mark credential number, and it is two options**.** There is the existing standard that has been in place for 10-15 years, which is the system code and credential number and then there is the next generation, which is the global unique identifier. You will hear more about that from Dwayne in his next presentation, but there are other issues, thinks like the employee number. How do I know who I am talking about? This is combined in the _____ as part of the _____, that is part of the legacy behavior. It is the person identifier field. So, this may be one of the more important pieces when I want to know, within the federal enterprise, that Steve Howard is the same Steve Howard at DOD as he is at DHS. Because I want to have that linkage. I need to understand who we are. So that is the electronic data interchange person identifier as defined by DOD. Each agency is responsible for figuring out what they use in that field. The employee name; that is in the printed information buffer. That something, you know, I mean usually you ask for name, rank, and serial number, okay. So, I talked about the serial number, here is the name, it is in your printed information buffer. It is also printed on the card, makes it easy to find. So, who is the issuer? When we look at the requirements of registration, I really have three things going on; who am i talking about, the affiliation of what organization they are part of, and how do I know it is unique? So, who is the issuer is in two places. It is in the card holder unique ID and it is buried in the _____, and it is called the agency code, but who is the issuer is also defined by your PIV authentication certificate. So, you have two choices in terms of how you are going to figure out who issued this card. So, the expiration date of the credential, same problem, we have two different places to describe that, each one is authoritative, if one is earlier than the other, you got a dead card, but there are two places. The cardholder unique ID has an explicate expiration date and your PIV authentication certificate has an expiration date. We will have to look at both to determine if that is a valid card. During registration, how are we going to mitigate the risks of tampering and fraud and terrorist exploitation. Part of that is integrity. So, what are the tools available to prove that I have the right card in front of me, held by the right bearer. So, issue or integrity, did they really put this data on the chip or on the card. That is a significant question, because one of the attacks, if I am an interested party is I am going to copy your card. I am going to try and skim it and clone it and I am going to change the numbers and hopefully I will get bigger privileges. Well that is not a cool idea. So, the data model support is mitigating that. We have two or three different ways of doing that. First one is in the cardholder unique ID, it is a mandatory obligation that the issuer signs everything. You will have that plus the certificate that gives you the public key, so you can now verify. You also have the IKO compliant signature object that covers every buffer on this card. So, the printed information, the name, the cardholder unique ID, that is also protected. Individually signed objects, each biometric placed on the card and every certificate is individually signed. So, you have flexibility here. If you verify those signatures, you have trust in the issuer. If you do not verify those signatures, you are not real sure. Is this the real PIV chip. You have got two methods to solve this one. You have the PIV card authentication key or you have the PIV authentication key. In both instances you will be asked to sign a challenge. The card authentication key's job is only to prove that you have a valid card. The PIV authentication key does two things. It proves a valid card and it confirms the bearer of the card at the same time, because you had to enter a PIN to use it. You got choices there. Is this the rightful bearer of that PIV card. We have got a couple of capabilities. Using the card holder finger prints, it is intended according to the _____ one that will do a match two card biometric identifier that proves that the bearer is the rightful card holder. Basically match two card I read, I enter the PIN, I read the biometrics of the card, I do a live scan, and I compare. So, now I have got yet another mechanism that allows me to prove that that card belongs to that person. Verifying the signature of those fingerprints is also required here because you have to have trust in the issuer. We want to know that those fingerprints were not substituted. A lot of capabilities here. Now, we are going to move into after I have registered you, I have got two different models that I am working on. I am using physical access control and I am using logical access control. So, where is the stuff you need in order to take advantage of this credential for those scenarios. In physical access, I present a credential, so which one is asking for access, right. So, you will look at the cardholder unique ID and the primary fields that are buried in the federal agency's marked credential number that are very important are the agency code, the system code, and the credential number, without all three you do not have uniqueness of credentials across every issuing agency. Reasoning being that the agency code says that DHS issued it, but DHS can start a credential #1 should they choose to, well guess what, DOD might also start a credential

#1. So, if I do not have the agency code as part of this, I will not know that I will not get a duplicate. Most definitely, we do not want Donald Rumsfield being credential #1 and all of a sudden he gets into every building as credential #1 and we certainly do not want the reverse to be true. That would be a lot more fun for me. Other method, the new method, next generation, is to use the global unique ID. It is the next generation replacing the credential number. The IAB has been working for quite a while on that one and the target there is to use an IP version 6 address and Tim Balter has been very central on that process. One of the goals was to not create and all new numbering scheme that the federal government had to administer; that is painful. Another thing is that there is the goal to have large issuance capabilities and GUID helps that. So, the next question you will ask is okay, I have identified which credential I am talking to, but now I got to say, who is asking for access. I mean if we all just do flash pass then what we have done is we can hand out our credential to Jim Dray and Jim Dray can now leave the facility as me and come back in the facility as me. It is a great way to go get lunch, and I think a lot of us have experience in that area. So, the next one is who is asking for access and that is bearer identification. You have a couple of tools. You have got the card holder fingerprints do to match two card. We also have the facial image in the printed information. Depends on the method that you are going to use at that gate or that entrance. Are you going to have a guarded man system and they are going to electronically pull the data off the chip and see it, that is one method, another is to require in the unattended scenarios, where I wave the card and I put my finger down, that is another method. You have got a range of options that will soothe the needs of you facility security plan based on what this card offers you. Next one is, is that card authentic. When I actually do the physical access transaction, there are two halves to this problem. The first one is the decision that has to be determined by the capability of the physical access control system you install. How often is it going to check to see if that card has been revoked, and Mr. Lee did a great job taking about the revocation transactions and the design of the system architecturally that supports the ID management talking to the back-end physical access control system. So, that is one method. Another method is lets just verify the signatures on that card, as appropriate to the transaction you are trying to do right there at the head-end, right there in the door reader or maybe at the access control panel. Those are methods that we need to start looking at because we certainly do not want cloned cards or modified cards to be enabled to get into buildings and facilities over time. That is a risk we want to start to mitigate, and then is this a copy, is this a cloned card or is it the real card. So, one of the key methods there is to use cryptographic challenge response. Use that card authentication key and challenge it for a digital signature. Logical access, okay. This question was asked by Tim, it has been asked by several people. I am just going to map it really easily, as far as I see it. The PIV authentication key, its origin, and the way it is actually designed. It is the same thing that is used in the DOD common access card and the NASA card for logical access. That is your logical access key, same one. Optionally, we can have the digital signature key that requires a PIN always for non-repudiation key management key, which allows you to establish E-mail encryption and session keys for SSL or VPN sessions; and then we have the card authentication key, which is to trust the card before doing any thing else. All of these things are consistent with DOD PKI key usage and that was very strategic. We wanted to make sure that all of the investment and how your business applications work today when you are talking about PKI are going to carry forward into the PIV domain.

QUICK SUMMARY:

So, here what we have done is _____ what data model enables to establish trust in the identity of the bearer of the token. You have got a range of possibilities for logical and physical access control and registration models. They are very heavily dependent on your agency's requirements for physical security and logical security. These transactions can go between the facility and the system and the network, and all of these things need continued focus, because I believe that from the interpretation of PIV, our goal is to maximize the potential of the use of this credential and that really needs focussing on the transactions and the methods to guarantee interoperability.

Thankyou.

Thanks Steve. Now, after all _____ what is all these mean in terms using this PIV card in a physical access system. _____.

This is the data model that Steve mentioned earlier. In the physical access world, the data element that _____ data model that is used in physical access is the Cardholder Unique ID. What is in this Cardholder Unique ID? These are the elements that are in it,. It has a FASC-N, the Federal Agency's Smart Credential Number, the Global Unique ID number, the expiration date, the authentication key map, which is optional. At this point, I would like to mention also that the Global Unique ID is also at this time is required to have, you can populate _____ signature and the agency code.

What is the Federal Agency Smart Credential Number? What is in it? As Steve mentioned, the elements of it are the agency code, the system code, the credential number, the credential series, and issue code most likely.

In addition to that there are personal identification number in the DOD world this is the ETI, PI number, it could be an employee number. In the earlier GSCIS specifications, we use the SEIWG number, which is the predecessor to FASC-N and in that case they originally use the Social Security Number, which obviously with some privacy issues involved there.

The next element is the Global Unique ID, as Steve mentioned is an IPv6 number, I am wondering what is that? Well. It's a very large number. It's sixteen digits that equate to 128 bits of information, the block of numbers can be obtained by an issuing agency and then issued out to the various smart cards. This will allow more _____ larger number, easier to mange numbering scheme as in the FASC-N number today, which _____ may know that the agency code in the FASC-N number is a kind of an issue at this point. The agency code is to be derived from a FIPS 95-2, which now is kind _____ supporting that.

The other elements of the Global Unique ID are the expiration date, which Steve mentioned is one of two places where the expiration date of the card itself, the credential itself is located. The other is in the certificate. Then the authentication key map - This is specified in the technical information guidance version 2.2 that the Inner Agency Advisory Board physical access working group graded and it was published last summer and that specifies way to use symmetric keys to authenticate the card _____ response mechanism. The final element is the issuer's asymmetric signature and digital signature of the entire _____, which validates that all of the information that included in the _____ has not been altered.

The devices that are required, now you have this card with all this information on it again in the physical access world, we were talking about using the information that is included in the _____. The device out there in the physical access system that is involved with this reading this card, obviously is the card reader. What is required of this card reader in terms of reading a PIV, well you are going to need a card reader that is an intelligent card reader that can actually read and process the _____ information. The specifications for the contact list card _____ the ISO 14443 specification and the contact card _____ ISO 7816 and that they will be able to process the _____. The specification of the all other documentations today did not specify the communication inner phase between the reader and the panel that's left up to the actual physical access control system at this point. After being able to read and process _____ information has to go finest way back to the access control system, which makes the intelligent decision to allow or deny access to the facility. Currently, to utilize this PIV card information in a physical access system, as Steve mentioned earlier, minimally to insure the URE dealing with a unique number you have to at least be able to process the agency code, the system code, the credential number that included in the _____. In addition, we will be able to validate the expiration date of that _____. Moving forward, intention is to move to this Global Unique ID and the migration to that in the future is going to be required by the smart card readers and the panels. As was you know who deal in the physical access control system is the access control panel, that is out in the facility that is controlling access to the doors on real-time basis and they communicate back to _____ house server and that house server has to be able to process the same information that the access control's panel processes. Again, _____ expiration date, migration, moving forward, Global Unique ID and then future for more _____. Right now at a minimum during the registration process, need to be able to validate the issue or signature before you enroll that credential number, PIV card into your physical access system. Moving forward potentially it gives that capability all the way out of the panel.

MALE VOICE I: Other options that are available is the DIF Card is the PIN Number. If a PIN is going to be used in junction with DIF Card Reader, FIPS-201 requires that the PIN pad be integrated with the reader to allow communication of that PIN directly to the card without having to be processed with some other external location. I heard some talk about the biometrics. As you mentioned earlier about the fact that the SP 800-76, which is going to answer the questions about whether the fingerprint biometric that stored on the card is going to be either an image or a template of some _____ template. There is host of products out in the market today that use fingerprints in physical access, so they are not interoperable. So prior to SP876 being issued and products being _____ to meet that requirement, you can use the biometrics in your Physical Access System for local use only and can guarantee inoperability at this point. After SP-876 is out there and products are available _____ interoperability, at that point. To verify the issue or signature requires obviously interface back to the CA or certificate replication list or an OCSP, online certificate status responder _____.

As ____ mentioned earlier, the Smart Card Alliance has established Physical Access Council _____Vice Chair of the Council. It is an industry government collaboration to work towards the understanding of how these government standards can _____ and what we are doing right now _____.

The Physical Access Council Steering Committee is made up of members from across the industry, government.

Here is just a list of some of the members of the Physical Access Council at this point. It probably does not include all of the members that since every day we have additional folks wanting to join this council and to become part of this, so as you can see there is voice support from industry to support this FIPS-201, HSPD-12 initiative and we are out there to build products that _____. Thank you and ____.

____ from one or two questions in a closing statement from you.

MALE VOICE II: Yeah just a quick closing statement from me in the 45 minutes that we had here to present this. I hope that the message you heard was that in the street does have now a road map to go for transitional product solution and endpoint product solution. The security issues relative to Physical Access and Logical Access are now doable under this framework and that we are actively working witnessed to try to solve the same issues and questions that you have about implementation, so that we make sure that we have a smooth transition to get you to these new product levels**.** With that we have time for a couple of questions ____

MALE VOICE I: Let me start with another thing just _____ in John.

MALE VOICE II: Sure**.**

MALE VOICE I: _____. There are some logistic issues they should be aware of. _____ getting back in.

MALE VOICE II: _____ but the other thing if you receive a little building _____ in your pocket **(VERY LOW VOICE) _____**

MALE VOICE I: Much quicker.

MALE VOICE II: Just one other thing that is John _____ did not sign up with the IAB that is John ____. I am just getting your contact information and John will make sure the you get the invite to the IAB _____ since he has been around this industry probably longer than anybody else, just let me ask the question knowing what Jim and I think Jim just walked up _____ there is a question this morning asked by _____ about the State of Affairs of the industry especially to PIV2 Compliant Technology. You know I think one of the questions in his room has been asked several different times in several different ways to your best of your knowledge understanding that to get to that compliant technology requires more than just vendors. There is _____ other things when would you believe that we will have that kind of products available if you would just try to guess.

MALE VOICE I: _____ question is a part I am not sure about. The rest of the question, _____ products out there.

MALE VOICE II: Yes.

MALE VOICE I: Are they used in millions.

MALE VOICE II: No.

MALE VOICE I: Have we experienced all the legal details of how they are going to work _____ operate.

MALE VOICE II: No.

MALE VOICE I: It is just like buying the card the first year it gets out.

MALE VOICE I: How do you verify that it interoperates, it is stable and so forth.
We have not been through that yet. Now when the products are going to be available and it is when the products are going to be qualified and certified and that is really where the issue. You will have to go ____ 140 that is time. That is _____ product I do not know and that is why I could not answer your question.

MALE VOICE II: Would you believe that the State of Affairs _____ Card Technology _____ available now ________ down the road, so that we can get only the policy process and culture change issues.

MALE VOICE I: I think to date it would be possible to cards to play with, not cards to issue immediately, but at least to start understanding how it goes, you will _____ products available, you will be able to build some elements. I know couple of them, which are nearly ready, but again the qualification product, it is something _____ card in your hand. It is another thing to issue a million of them and that is were the issue is going to be.

LADY VOICE: My name is _____. I am from the Department of Commerce. I have a question specifically about the digital signature _____ clarification one of the slides for the Physical _____ digital signature. I am able to state that a digital signature is required for Physical Access for ICC integrity, but it is optional for Logical Access. I was wondering why is it optional for logical and mandatory for physical.

MALE VOICE I: That is a appropriate question. It is actually really what we are trying to do is make sure they were capable of doing _____ technology service meeting public key technology services, no matter which environment you are in and in the logical environment using the existing PIB authentication key, _____, you got it. It is absolutely a required PKI authentication mechanism for Logical Access. The whole was what we do about Physical Access. So the card authentication key is an addition to those data models to enable that to be used in that environment. It is not exclusive. You could choose to use the existing PIB authentication key with a PIN and a Physical Access control environment.

MALE VOICE II: You guys are happy to know that I got two pages of questions one _____

MALE VOICE I: Laughing …….

MALE VOICE II: _____

MALE VOICE I: One final comment resources. Okay everybody wants more resources and the Smart Card Alliance that were at web site, which is up there. We have five papers that are relative to PIV an implementation of Smart Cards. They were available for free to all government members. You just need to send an e-mail to info@smartcardalliance.org and we would be happy to send them. Enjoy your lunch. We will see you back at 1:00.